第 28 卷 第 2 期 2007 年 2 月
井冈山学院学报(自然科学) Journal of Jinggangshan University(Natural Sciences)
Vol.28 No.2 Feb.2007

初等数论中蕴涵的数学思想方法

王丹华, 杨海文

(井冈山学院 数理学院, 江西 吉安 343009)

[摘要] 以初等数论中著名的 Euler 与 Wilson 定理证明为切入口, 探讨初等数论中蕴涵的整体化、配对、化归数学思想方法。

[关键词] 初等数论; 数学思想方法; 蕴涵

[中图分类号] G642 [文献标识码] B [文章编号] 1673-4718 (2007) 02-0020-02

初等数论以整除和同余理论为基础,主要研究整数性质和不定方程。初等数论貌似简单,但真正掌握并非易事,它的内容严谨简洁,方法奇巧多变,蕴含了丰富的数学思想方法, 其数学思想方法又往往隐含在数学知识形成和问题解决的过程中。下文以初等数论中著名的 Euler 与 Wilson 定理证明为切入口, 例谈初等数论中解题过程中蕴涵的整体化、配对、化归思想方法。

1 整体化思想方法

Euler 定理 [1]: '设 m是大于 1 的正整数, a 是任意整数,且 $(a,m)=1$, 则 $a^{\phi(m)}\equiv 1(\mathrm{mod}\ m)$。"

证明: 若 $r_1,r_2,\cdots,r_{\phi(m)}$是模 m的简化剩余系, $(a,m)=1$, 则 $ar_1,ar_2,\cdots,ar_{\phi(m)}$也是模 m的简化剩余系, 从而 $ar_1\cdot ar_2\cdots ar_{\phi(m)}=r_1\cdot r_2\cdots r_{\phi(m)}(\mathrm{mod}\ m)$, 即 $a^{\phi(m)}\cdot r_1\cdot r_2\cdots r_{\phi(m)}\equiv r_1\cdot r_2\cdots r_{\phi(m)}(\mathrm{mod}\ m)$, 由此及同余性质得: $a^{\phi(m)}\equiv 1(\mathrm{mod}\ m)$。

注意到, Euler 定理的证明虽然十分简单, 但它揭示了重要的数学思想方法—— '整体化思想方法"。整体化思想方法就是把单个对象始终放在整体对象构成的系统中加以考察, 通过系统对象之间的整体联系或整体特征, 寻求原问题的解决途径。从以上的证明过程知道, Euler 定理的证明依赖于模 m的简化剩余系的整体性质: '若 $r_1,r_2,\cdots,r_{\phi(m)}$是模 m的简化剩余系, $(a,m)=1$, 则 $ar_1,ar_2,\cdots,ar_{\phi(m)}$也是模 m的简化剩余系, 且模 m的任一简化剩余系中所有数的乘积模 m都同余"。类似地, 设 $a_1,a_2,\cdots,a_m$为模 m的完全剩余系, 则 a_i 与且只与某一个 $i(1\le i\le m)$同余, 由此可得到完全剩余系的整体性质: $\sum_{i=1}^{m} a_i^n=\sum_{i=1}^{m} i^n(\mathrm{mod}\ m)$, $(n\in N)$等。利用模 m的完全剩余系(或简化剩余系)的整体性质, 就可以另辟蹊径, 获得巧妙简捷的解(证)题效果。

例 1 设 p 为奇素数, n 为正整数, $2^n\not\equiv 1(\mathrm{mod}\ p)$, 证明: $1^n+2^n+\cdots+(p-1)^n\equiv 0(\mathrm{mod}\ p)$

证明: 由 $1,2,\cdots,(p-1)$是模 p 的一个简化剩余系, $(2,p)=1$, 可知 $2\cdot 1,2\cdot 2,\cdots,2\cdot(p-1)$也是模 p 的一个简化剩余系, 再由简化剩余系的整体性质可得:

$1^n+2^n+\cdots+(p-1)^n\equiv(2\cdot 1)^n+(2\cdot 2)^n+\cdots+(2\cdot(p-1))^n\ (\mathrm{mod}\ p)$.

上式即: $(2^n-1)\cdot(1^n+2^n+\cdots+(p-1)^n)\equiv 0(\mathrm{mod}\ p)$, 又

$\because 2^n\not\equiv 1(\mathrm{mod}\ p)$.

$\therefore 1^n+2^n+\cdots+(p-1)^n\equiv 0(\mathrm{mod}\ p)$.

利用例 1 及模 m简化剩余系的整体性质可证明如下更一般的结论:

设 p 为奇素数, 2 为 p 的原根, $S_n=\sum_{k=1}^{p-1} k^n$, $(n\ge 1, n\in N)$, 则 $n\not\equiv 0(\mathrm{mod}(p-1))$时, $S_n\equiv 0(\mathrm{mod}\ p)$; $n\equiv 0(\mathrm{mod}(p-1))$时, $S_n=-1(\mathrm{mod}\ p)$(证明略)。

2 配对思想方法

Wilson 定理[2]: 设 p 是素数, 则 $(p-1)!\equiv -1(\mathrm{mod}\ p)$.

证明 $p=2$ 时结论显然成立。设 p 是奇素数时, 对每一个整数 $a(0<a<p)$, 存在惟一的整数 $a'(0<a'<p)$, 使得 $a\cdot a'\equiv 1(\mathrm{mod}\ p)$; 如果 $a=a'$, 则 $a^2\equiv 1(\mathrm{mod}\ p)$, 这时 $a=1$ 或 $a=p-1$, 除此之外, 剩下 $p-3$ 的个数$\{2,3,\cdots,p-2\}$按关系式 $a\cdot a'\equiv 1(\mathrm{mod}\ p)$可配成 $\frac{p-3}{2}$ 对, 于是有 $2\cdot 3\cdots(p-2)\equiv 1(\mathrm{mod}\ p)$, 故 $(p-1)!\equiv 1\cdot 2\cdot 3\cdots(p-2)\cdot(p-1)\equiv(p-1)\equiv -1(\mathrm{mod}\ p)$。

Wilson 定理证明过程蕴涵了数学思想方法—— '配对思想方法"。配对的思想方法就是将整体对象中的满足某种特性的对象进行组合配对, 再利用配对后的特性解决原问题。初等数论中有许多配对的情形存在。如:

①若 $(a,m)=1$, 则 $(m-a,m)=1$, 即 a 与 m-a 同属于模 m的简化剩余系;

②若 d 是正整数 n 的正因数, 则 d 与 $\frac{n}{d}$ 同为正

收稿日期: 2006-09-04
作者简介: 王丹华(1953-), 女, 江西吉安人, 教授, 主要从事初等数论的教学与研究.

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

整数 n 的正因数;

③若 $p\equiv1(\mathrm{mod}4)$, 则 r 与 p-r 同为模 p 的平方剩余或同为平方非剩余。

例 2 若 p 为素数, $p\equiv1(\mathrm{mod}4)$, 证明 $\sum_{r=1}^{p-1} r\cdot(\frac{r}{p})=0$, 其中 $(\frac{r}{p})$ 是 r 对模 p 的 Legendre 符号[3]。

证明: $\because p\equiv1\ (\mathrm{mod}4)$, $\therefore (\frac{-1}{p})=1$, 于是可推出 $(\frac{p-r}{p})=(\frac{r}{p})$, 由此可知, r 与 p-r 同为平方剩余或同为平方非剩余。令 $p=4n+1$, 则对模 p 而言有 2n 个平方剩余及 2n 个平方非剩余。根据这一点, 对任一 r, $(1\le r\le p-1)$, 将 r 与 p-r 配成一对, 则 2n 个平方剩余可配成 n 对, 2n 个平方非剩余也可配成 n 对, 故 $\sum_{r=1}^{p-1} r\cdot(\frac{r}{p})=np+(-np)=0$。

3 化归思想方法

化归是一种常用的数学思想方法。化归是指问题之间的相互转化, 或者将问题的一种形式转换成另一种形式, 或者把复杂问题转化成较简单问题、将陌生问题转化为已经解决问题或熟悉问题。通过恰当的化归转换不仅能够顺利地解决原问题, 而且有助于培养学生科学的思维习惯。初等数论中主要化归思想方法有: 变形化归、分割化归、映射化归等[4]。

在初等数论中, 利用 "$b\mid a\Leftrightarrow a=bq+r(0\le r\le|b|)$ 中的 $r=0$", 整除可以等价化归为带余数除法问题; 利用 "$m\mid a\Leftrightarrow a\equiv0(\mathrm{mod}\ m)$" 或 "$a\equiv b(\mathrm{mod}\ m)\Leftrightarrow m\mid(a-b)$", 整除与同余问题可以相互等价化归; 不定方程也常常化归为同余问题求解。通过适当的(等价或不等价)化归, 使解(证)题思路更清晰, 计算、证明过程更简捷, 起到殊途同归的效果。初等数论中有关化归思想方法的例(习)题俯拾即是, 限于篇幅, 此处从略, 下面仅综合考察合数模 m 的同余式求解过程中的化归思想方法。

例 3 $f(x)\equiv0(\mathrm{mod}\ m)\cdots(*)$ 求解过程中的化归思维[4]:

①利用算术基本定理将合数模 m 化归为标准分解式:

$m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, $(p_1<\cdots<p_k,\ \alpha_i>0,\ \alpha_i\in N, i=1,2,\cdots,k, p_i$ 是素数);

②将同余式(*)化归为等价素数幂模的同余式组:

$f(x)\equiv0(\mathrm{mod}\,p_i^{\alpha_i}),(i=1,2,\cdots,k)\cdots(**)$;

③素数幂模同余式 $f(x)\equiv0(\mathrm{mod}\,p_i^{\alpha_i})$ 化归为依次求解同余式: $f(x)\equiv0(\mathrm{mod}\ p_i)$, $f(x)\equiv0(\mathrm{mod}\ p_i^2)$, $\cdots$, $f(x)\equiv0(\mathrm{mod}\ p_i^{\alpha_i-1})$ 的基础上, 最后求出(**)中每一个同余式: $f(x)\equiv0(\mathrm{mod}\ p_i^{\alpha_i})$, $(i=1,2,\cdots,k)$ 的 t_i 个解;

④对于(**)每一个同余式的 t_i 个解 $x\equiv S_{ij_i}(\mathrm{mod}\ p_i^{\alpha_i})$, $(1\le j_i\le t_i)$, 通过变形化归为与原同余式(*)等价的同余式组: $x\equiv S_{ij_i}(\mathrm{mod}\ p_i^{\alpha_i})$, $(i=1,2,\cdots,k,\ 1\le j_i\le t_i)$, 再利用孙子定理求出每一个同余式组的解, 从而求得原同余式(*)的 $T=t_1t_2\cdots t_k$ 个解。

4 结束语

初等数论解题过程中除了以上探讨的整体化、配对、化归数学思想方法, 还涉及其它的数学思想方法(如: 构造思想, 分类思想等)。值得注意的是, 初等数论解(证)题往往是多种数学思想方法相互交织、渗透、化归的综合应用过程。如: 在例 2 中, 首先是将问题化归为 "$p\equiv1(\mathrm{mod}4)$ 条件下, r 与 p-r 同为平方剩余或同为平方非剩余" 问题, 其次再依据 "r 与 p-r 是否同为平方(平方非)剩余" 考虑配对问题), 从某种意义上来讲, 配对的思想方法实质上是局部整体化思想方法的变形, 同时也是整体化归为部分思想的体现, 而例 3 的解题过程则体现了中化归思想方法的综合应用。

初等数论中蕴含了丰富的数学思想方法, 其知识结构和数学思想方法形成一个经纬交织, 融会贯通的知识网络, 需要我们去挖掘、揭示。因此, 在初等数论的教学过程中, 应充分利用教材和习题的教育功能, 注重展示解决问题的思路、思维过程, 体现解决问题策略与方法的多样性, 引导沟通知识间的内在联系, 突出问题的背景和思想方法的阐述, 注重数学思想方法的总结、提炼, 把数学知识和相关数学思想方法有机联系起来, 使学生从整体上把握初等数论的理论体系, 理解数学思想方法的内涵, 开阔思维视野, 健全认知结构。

参考文献

[1]于秀源,瞿维建.初等数论[M].济南:山东教育出版社,2001.66-68.

[2]潘承洞,潘承彪.初等数论[M].北京:北京大学出版社,1999.144-145.

[3]闵嗣鹤,严士健.初等数论[M].北京:高等教育出版社,2003.91-95.

[4]王丹华,杨海文.'初等数论'中的化归思维方法[J].井冈山学院学报(自然科学),2006,(2):14.

(下转第 24 页)

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

的,…。

参考文献

[1]徐俊明.图论及其应用[M].合肥:中国科学技术大学出版社,2004.

[2]俞万禧.2t名运动员的循环赛和对集的划分[J].安徽理工大学学报(自然科学版),2006,26(1):64- 69.

[3]俞万禧.对集的划分与循环赛的安排[J].阜阳师范学院学报(自然科学版),2006,22(4):8- 12.

Round- robin tournaments and duplet sets algorithm

CHOU Wan- xi

(Dept of Civil Engineering, Anhui University of Science and Technology, Huainan 232001, China)

Abstract:The definitions about edge matrix and round- robin tournament are given. An slgorithm of determining duplet sets of the complete graph and a method of constructing round- robin tournaments without duplet sets in common are proposed. The emuration problem of any duplet set and round- robin tournament is discussed. The construction procedure of round- robin tournaments without duplet sets in common is presented.

Key words:duplet set; complete graph; edge matrix; round- robin tournaments; algorithm

(责任编辑:彭晓冬)

(上接第21页)

Mathematical thoughtway in elementary number theory

WANG Dang- hua, YANG Hai- wen

(Department of Math and Physics, Jinggangshan University, Ji'an 343009, China)

Abstract:The article discuss whole, partnership and change mathematical thoughtmethod According to famous the Euler theory and the Wilson theory in elementary number theory.

Key words:elementary number theory; mathematical thoughtway; contain

(责任编辑:彭晓冬)

© 1994-2009 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net